

IN THE CLAIMS

The following is a listing of the claims in the application with claims 1, 4-8, 10-18 and 19-53 shown as amended and claims 2-3, 9 and 19-20 cancelled.

LISTING OF CLAIMS

1. (currently amended) Method for an operator to dynamically and remotely control the pairing of digital data reception equipment (2) with a plurality of one or more external security modules (6, 8) each having a unique identifier and with each security module being adapted to cooperate with said digital data reception equipment for controlling reception of distributed data by means of said digital data reception equipment (2) and with the digital data reception equipment having a computer and a stored program, ~~method characterised in that it comprises said method comprising~~ the following steps:

using the computer to verify whether or not the identifier of said external security modules (6, 8) is memorized in the digital data reception equipment (2), upon connection of said external security modules (6, 8) connecting an external security module (6, 8) to the digital data reception equipment, and

if the unique identifier of the external security modules (6, 8) is memorized in the digital data reception equipment (2), transmitting a control signal to the digital data reception equipment (2) defining configuration parameters to activate the pairing of said digital data reception equipment (2) with said external security modules (6, 8), and

if the unique identifier of the external security modules (6, 8) is not memorized

in the digital data reception equipment (2), transmitting a control signal to the digital data reception equipment (2) defining configuration parameters to deactivate the pairing of said digital data reception equipment (2) with said external security modules (6, 8).

~~— memorizing, on the fly, the unique identifier of the connected security module (6, 8) in the reception equipment (2).~~

Claims 2-3 (cancelled).

4. (currently amended) ~~Method~~ The method according to claim 3 ~~1,~~
characterised in that ~~wherein~~ said configuration parameters ~~signal includes~~ include
at least one of the following ~~instructions~~ functional parameters:

- ~~[-]~~ authorizing ~~memorization~~ memorization,
- ~~[-]~~ prohibiting ~~memorization~~ memorization,
- ~~[-]~~ erasing identifiers previously ~~memorised~~ memorized in the digital data reception equipment (2),
- ~~[-]~~ activating or deactivating ~~the~~ a verification phase including a procedure consisting of disturbing the data processing if the identifier of the connected external security module (6, 8) is not previously memorized in the digital data reception equipment (2).

5. (currently amended) ~~Method~~ The method according to claim 3 ~~1~~, characterised ~~wherein~~ said control signal also includes an indication as to the maximum allowable number of ~~memorised~~ identifiers to be memorized in the digital data reception equipment (2).

6. (currently amended) ~~Method~~ The method according to claim 3 ~~1~~, characterised ~~in that~~ ~~wherein~~ said signal configuration parameters includes a reconfiguration instruction through which an updated list of identifiers of external security modules (6, 8) paired with the digital data reception equipment (2) is transmitted to said digital data reception equipment (2).

7. (currently amended) ~~Method~~ The method according to claim 6, characterised ~~wherein~~ ~~in that~~ said updated list of identifiers is transmitted directly to the digital data reception equipment (2).

8. (currently amended) ~~Method~~ The method according to claim 6, characterised ~~wherein~~ ~~in that~~ said updated list of identifiers is transmitted through ~~an~~ the external security module (6, 8) connected to said digital data reception equipment (2).

9. (cancelled).

10. (currently amended) ~~Method~~ The method according to claim 1, ~~characterized~~ ~~wherein~~ ~~in that~~ said distributed data ~~are~~ is either unencrypted or is encrypted by means of an encrypted control word and in that each external security module (6, 8) includes access rights to said data and a decryption algorithm for said control word.

11. (currently amended) Method The method according to claim 4, characterized ~~wherein in that~~ said signal configuration parameters are is transmitted to a the digital data reception equipment (2) in an EMM message specific to an external security module (6, 8) associated with said digital data reception equipment (2).

12. (currently amended) Method The method according to claim 4, characterized ~~wherein in that~~ said configuration parameters are ~~signal~~ is transmitted to a digital data reception equipment (2) in an EMM message specific to said digital data reception equipment (2).

13. (currently amended) Method The method according to claim 6, characterized ~~wherein in that~~ for a given digital data reception equipment (2), said updated list of identifiers is transmitted in an EMM message specific to a security module (6, 8) associated with this digital data reception equipment (2).

14. (currently amended) Method The method according to claim 4, characterized ~~wherein in that~~ said configuration parameters are ~~signal~~ is transmitted to a group of digital data reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said digital data reception equipment (2).

15. (currently amended) Method The method according to claim 4, characterized ~~wherein in that~~ said configuration parameters are ~~signal~~ is transmitted to a group of digital data reception equipment (2) in an EMM message specific to said group of digital data reception equipment (2).

16. (currently amended) Method The method according to claim 6, characterised ~~wherein in that~~ for a given group of digital data reception equipment (2), said updated list of identifiers of external security modules (6, 8) is transmitted in an EMM message specific to a said given group of external security modules (6, 8) associated with said digital data reception equipment (2).

17. (currently amended) Method The method according to claim 4, characterised ~~wherein in that the~~ configuration parameters for the verification phase are message for managing the verification phase is transmitted to a group of digital data reception equipment (2) ~~in a private flow processed by using [a]~~ dedicated software executable in each digital data reception equipment (2) ~~according to as a function of the~~ identifier of the external security module associated with said digital data reception equipment.

18. (currently amended) Method The method according to claim 6, characterised ~~wherein in that~~ for a given group of digital data reception equipment (2), said updated list of identifiers of external security modules (6, 8) is transmitted to each digital data reception equipment (2) in a private flow processed by a dedicated software executable in each digital data reception equipment according to as a function of the identifier of the external security module associated with said digital data reception equipment.

Claims 19–20 (previously cancelled).

21. (currently amended) Method The method according to claim 11, ~~characterised~~
~~wherein in that~~ said EMM message consists of ~~contain messages with~~ the following
 structure format:

EMM-U_section() {	
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_address_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

22. (currently amended) Method The method according to claim 14, ~~characterised~~
~~in that wherein~~ said EMM message is specific to all external security modules (6, 8)
 or to all digital data reception equipment (2) and ~~contain messages with~~ consists of
 following structure format:

EMM-G_section() {	
table_id = 0x8A or 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-G_section_length	12 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

23. (currently amended) Method The method according to claim 14, characterised in that wherein said EMM message is specific to a sub-group of external security modules (6, 8) or digital data reception equipment (2) and ~~contain messages with~~ consists of the following structure format:

EMM-S_section()	{	
table_id = 0x8E		8 bits
section_syntax_indicator = 0		1 bit
DVB_reserved		1 bit
ISO_reserved		2 bits
EMM-S_section_length		12 bits
shared_address_field		24 bits
reserved		6 bits
data_format		1 bit
ADF_scrambling_flag		1 bit
for (i=0; i<N; i++) {		
EMM_data_byte		8 bits

24. (currently amended) Method The method according to claim 1, characterised in that wherein the identifiers of the external security modules (6, 8) are grouped in an encrypted list.

25. (currently amended) Method The method according to claim 1, characterised in that wherein the digital data reception equipment (2) includes a decoder and the external security modules (6, 8) includes an access control cards (6) in which information about access rights of a subscriber to digital data distributed by an operator is ~~memorized~~ memorized, and in that pairing is done between said decoder and said access control cards (6).

26. (currently amended) Method The method according to claim 1, characterised in that wherein the digital data reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory that can cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that wherein pairing is done between said decoder and said removable security interface (8).

27. (currently amended) Method The method according to claim 1, characterised in that wherein the digital data reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory that can cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), and in that wherein pairing is done between said removable security interface (8) and said access control cards (6).

28. (currently amended) Method The method according to claim 10, characterised in that wherein the data are audiovisual programs.

29. (currently amended) Digital data reception equipment (2) for pairing to one or more that can be paired with a plurality of external security modules (6, 8) each having a unique identifier to manage access to digital data distributed by an operator, characterised in that it includes comprising means for executing a computer program stored in a readable medium for: ~~memorizing on the fly, the identifier of each external security module (6, 8) connected to said reception equipment.~~

verifying whether or not the identifier in said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment,

activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2), and

deactivating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already memorized in the digital data reception equipment (2).

30. (currently amended) The digital data reception equipment according to claim 29, ~~characterised in that it comprises~~ further comprising a decoder and ~~in that wherein~~ the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, pairing being done between said decoder and said access control card (6).

31. (currently amended) The digital data reception equipment according to claim 29, ~~characterised in that it includes~~ further comprising a decoder and ~~in that wherein~~ the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and that is designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, pairing being done between said decoder and said removable security interface (8).

32. (currently amended) The digital data reception equipment according to claim 29, ~~characterised in that it includes~~ further comprising a decoder provided with a removable security interface (8) with a non-volatile memory ~~and that is~~ designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards (6) and ~~in that wherein~~ pairing is done between said removable security interface (8) and said access control cards (6).

33. (currently amended) ~~A Decoder~~ decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a unique identifier and including at least one data processing algorithm, with said decoder ~~characterised in that it includes~~ comprising means responsive to said data processing algorithm for memorizing, ~~on the fly, the identifier of each external security module (6, 8) connected to said decoder.~~ executing orders sent by the operator for:

verifying whether or not the identifier of said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment.

activating the pairing of said digital data digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2), and

deactivating the pairing of said digital data reception equipment (2) with said

external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is not already memorized in the decoder.

34. (currently amended) ~~The Decoder~~ decoder according to claim 33, characterised in that ~~wherein~~ said external security modules (6, 8) are access control cards (6) in which are stored information about access rights of a subscriber to digital data distributed by an operator.

35. (currently amended) ~~The Decoder~~ decoder according to claim 33, characterised in that ~~wherein~~ said external security modules (6, 8) are removable security interfaces (8) including a non-volatile memory that can cooperate firstly with the decoder and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator.

36. (currently amended) ~~Reception equipment comprising a removable~~ Removable security interface (8) including a non-volatile memory designed to cooperate firstly with a digital data reception equipment (2) having a decoder and secondly, having a plurality of conditional access control cards (6), to manage access to digital data distributed by an operator, each access control card (6) having a unique identifier and containing information about access rights of a subscriber to said digital data, with said removable security interface characterised in that it includes further comprising means for recording the identifier of each access control card (6) in said non-volatile memory, ~~on the fly, and at least one data processing algorithm for use by said decoder to activate or deactivate the pairing of the~~ reception equipment to the control cards.

37. (currently amended) ~~The removable security interface~~ Reception equipment according to claim 36, ~~characterised in that it consists of~~ comprising a PCMCIA card on which is installed digital data descrambling software.

38. (currently amended) ~~The removable security interface~~ Reception equipment according to claim 36, ~~characterised in that it~~ which consists of a software module.

39. (currently amended) An Executable executable computer program stored in a computer readable medium of a digital data reception equipment (2) that can cooperate with a plurality of external security modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, said digital data reception equipment (2) comprising a computer for executing said executable computer program, ~~characterised in that it wherein the executable computer program~~ includes instructions for: ~~executing the memorization, on the fly, of the identifier of each external security module (6, 8) connected to said reception equipment (2),~~ verifying whether or not the identifier of said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment, activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is already memorized in the digital data reception equipment (2), and deactivating the pairing of said decoder with said external security modules (6, 8) if the unique identifier in the external security modules (6, 8) is not already

memorized in the decoder.

40. (currently amended) ~~The Computer~~ computer program according to claim 39, characterised in that it also includes further comprising instructions for locally generating pairing control parameters of the digital data reception equipment (2) with an external security module (6, 8) as a function of a control signal transmitted to said digital data reception equipment (2) by the operator.

41. (currently amended) ~~The Computer~~ computer program according to claim 39, characterised in that it also includes further comprising instructions for checking if the identifier of said external security module (6, 8) is ~~memorised~~ memorized in the digital data reception equipment (2), at each connection ~~later use of an~~ the external security module (6, 8) with the digital data reception equipment (2).

42. (currently amended) ~~A System~~ system including a plurality of comprising a management platform (1) and a digital data reception equipment (2) connected to a data and/or services broadcasting network for communication with the digital data reception equipment and with each the digital data reception equipment (2) adapted to be being paired with a plurality of external security modules (6, 8), ~~said system also including a commercial management platform (1) communicating with the reception equipment (2) and with said external security modules (6, 8) characterised~~ characterized in that it also includes each having a unique identifier, wherein the system further comprises:

[-] a first module arranged in said commercial management platform (1) ~~and that will generate~~ for generating pairing queries, and

[-] a second security module arranged in said digital data reception equipment (2) that will process the generated said queries from the first module to prepare a pairing configuration and to control said pairing, using pairing control parameters generated by a computer in said digital data reception equipment based upon verifying whether or not the identifier of said external security modules (6, 8) is already memorized in the digital data reception equipment (2) upon connection of said external security modules (6, 8) to the digital data reception equipment, activating the pairing of said digital data reception equipment (2) with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is already memorized in the digital data reception equipment (2), and deactivating the pairing of said decoder with said external security modules (6, 8) if the unique identifier of the external security modules (6, 8) is not already memorized in the decoder.

43. (currently amended) Method The method according to claim 5, characterised in that wherein said control signal is transmitted to a digital data reception equipment (2) in an EMM message specific to an external security module (6, 8) associated with said digital data reception equipment (2).

44. (currently amended) Method The method according to claim 5, characterised in that wherein said control signal is transmitted to a digital data reception equipment (2) in an EMM message specific to said digital data reception equipment (2).

45. (currently amended) ~~Method set forth in~~ The method according to claim 5, characterised in that ~~wherein~~ said control signal is transmitted to a group of digital data reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said digital data reception equipment (2).

46. (currently amended) ~~Method set forth in~~ The method according to claim 5, characterised in that ~~wherein~~ said control signal is transmitted to a group of digital data reception equipment (2) in an EMM message specific to said group of digital data reception equipment (2).

47. (currently amended) ~~Method set forth in~~ The method according to claim 5, characterised in that ~~wherein~~ the message for managing the verification phase is transmitted to a group of digital data reception equipment (2) ~~in a private flow processed by a~~ using dedicated software executable in each digital data reception equipment as a function of the identifier of the external security module associated with said digital data reception equipment.

48. (currently amended) ~~Method set forth in~~ The method according to claim 12, characterised in that ~~wherein~~ said EMM contain messages with message consists of the following format:

EMM-U_section() {	
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits

for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

49. (currently amended) Method set forth in The method according to claim 13,
~~characterised in that wherein said EMM contain messages with~~ message consists of
the following format:

EMM-U_section() {	
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

50. (currently amended) Method set forth in The method according to claim 15,
~~characterised in that wherein said EMM is specific to all external security modules~~
(6, 8) or to all digital data reception equipment (2) and contain messages with
consisting of the following structure:

EMM-G_section() {	
table_id = 0x8A or 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-G_section_length	12 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

51. (currently amended) Method set forth in The method according to claim 16,
~~characterised in that wherein~~ said EMM is specific to all external security modules
 (6, 8) or to all digital data reception equipment (2) and contain messages consisting
of with the following structure:

```

EMM-G_section() {
  table_id = 0x8A or 0x8B                8 bits
  section_syntax_indicator = 0            1 bit
  DVB_reserved                            1 bit
  ISO_reserved                            2 bits
  EMM-G_section_length                    12 bits
  for (i=0; i<N; i++) {
    EMM_data_byte                          8 bits
  }

```

52. (currently amended) Method set forth in The method according to claim 15,
~~characterised in that wherein~~ said EMM is specific to a sub-group of external
 security modules (6, 8) or digital data reception equipment (2) and contain
 messages with consisting of the following structure:

```

EMM-S_section() {
  table_id = 0x8E                          8 bits
  section_syntax_indicator = 0            1 bit
  DVB_reserved                            1 bit
  ISO_reserved                            2 bits
  EMM-S_section_length                    12 bits
  shared_address_field                    24 bits
  reserved                                6 bits
  data_format                            1 bit
  ADF_scrambling_flag                     1 bit
  for (i=0; i<N; i++) {
    EMM_data_byte                          8 bits
  }

```

53. (currently amended) ~~Method set forth in~~ The method according to claim 16, characterised in that ~~wherein~~ said EMM is specific to a sub-group of external security modules (6, 8) or digital data reception equipment (2) and contain messages with consisting of the following structure:

EMM-S_section() {	
table_id = 0x8E	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-S_section_length	12 bits
shared_address_field	24 bits
reserved	6 bits
data_format	1 bit
ADF_scrambling_flag	1 bit
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits